**Kryptos 2019**

**Challenge 1: Solution**

We need to decrypt the Username and Password for the Dirtydeeds website:

```
User:   QAZ QSZ QA WAZ WASZ QS QASZ QW QAZ Q WASX
Pass:   QW QSZ QWS QS QWZ QSZ QWSZ QZ QS QWSZX WAZ QASZ
        QZX WAZ
```

Observations and clues from the provided documents:

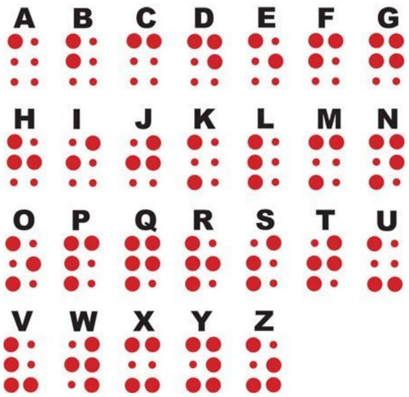
- The only letters used in the ciphertext are : Q,W,A,S,Z,X
- These letters are grouped on the left side of a standard QWERTY keyboard, roughly in three rows and two columns.
- Claudia Proust sometimes refers to herself as “lobsterclaw”, which has 11 letters.
- The usernames for Gmail1 and Dirtydeeds are the same, each with 11 groupings of letters.
- Claudia’s family moved to West Philadelphia so her sister could attend Overbrook School. A google search shows that there is an Overbrook School for the blind in West Philadelphia.
- Claudia has an account at a location she refers to “AFB”. While there is no afb.com website, there is an afb.org website. This is the American Federation for the Blind.

Depending on which clues one discovered, there are a variety of ways to solve this challenge. Three are outlined below:

**Solution 1**: There are several references to “blind”. Braille is the common written language for the blind. Letters in Braille are determined by raised patterns among six “dots” that are arranged in three rows and two columns (six dots). Therefore, the six ciphertext letters can take the place of “dots”. This conjecture can be confirmed by decrypting the phrase at the top of the PINS document, which turns out to be “Encrypted in Braille”. Using the Braille language (see below), one can decrypt the username and password for Dirtydeeds (or the rest of the PINS document).

Username: lobsterclaw

Password: codemonkeysrus



**Solution 2**: If we assume that the username for Dirtydeeds is “lobsterclaw” we can make the appropriate substitutions for each ciphertext grouping of letters and the corresponding plaintext letter:

QAZ – l

QSZ – o

QA – b

WAZ – s

WASZ – t

QS – e

QASZ – r

QW – c

QAZ – l

Q – a

WASX – w

Substituting these know CT/pt pairs into the phrase at the top of the PINS document yields:

```
e*cr**te*
   **
 *ra*lle
```

From here, one might guess the first word is “encrypted” and the last word is “braille”.  Once one knows it is encrypted using Braille, one can look up the table for letters in Braille and continue to decrypt the rest of the document with ease.

**Solution 3**: It is possible to decrypt the entire PINS document without ever making the connection that it is enciphered using Braille.  A couple of Kryptos Teams started with frequency analysis, made some reasonable educated guesses, and proceeded to just treat this as a simple substitution cipher.